Remarks

The Official Action rejected claims 1-34 and objected to the specification.

Applicant has amended the specification, has amended claims 3, 6-8, 13, 15-18, 22,

25-29 and 31, and has canceled claims 1, 14, 19-21 and 24. Claims 2-13, 15-18,

22-23, and 25-34 remain pending.

Specification Objections

The Official Action objected to the Abstract. Applicant respectfully disagrees

with the Official Action. The Abstract as filed satisfies all "requirements" under the

law. As indicated in the prior response, MPEP 608.01 provides guidelines for

drafting the Abstract. Almost all of these guidelines are drafted in permissive terms

such as "should" and thus are not "required". Requirements are often prefaced with

the words such as "must" or "shall". Applicant believes the Abstract satisfies all

"requirements". However, in the interest of expediting prosecution, Applicant has

amended the Abstract to include additional details.

If the Examiner elects to maintain the present objection, Applicant respectfully

requests the Examiner to indicate which "requirements" the Abstract fails to satisfy

and the information the Examiner would like to see added to the Abstract. To this

end, the Applicant respectfully requests the Examiner to provide precisely the

information the Examiner wants and not merely quote sections of the MPEP, CFR or

USC. Applicant respectfully requests the withdrawal of the present objection.

Claim Rejections - 35 USC § 102 (Davis)

The Official Action rejected claims 1-2, 6-9, 12-13, 19-21 and 29-34 under 35

USC 102(e) as being anticipated by Davis et al (US 6,401,208). Applicant has

canceled claims 1 and 19-21 and amended claims 6-8, 13, 29 and 31. Applicant

respectfully requests the rejection of claims 2, 6-9, 12-13 and 29-34 be withdrawn in

light of the following.

<u>Claims 2, 6-9, 12-13</u>

As a result of the present amendment, each of claims 2, 6-9 and 12-13

includes claim 3 as a base claim. Claim 3 was not rejected under Davis. Thus,

claims 2, 6-9 and 12-13 are allowable over Davis. Applicant respectfully requests

the present rejection of claims 2, 6-9 and 12-13 be withdrawn.

<u>Claims 29-34</u>

As a result of the present amendment, each of claims 29-34 requires a

machine readable medium comprising one or more instructions that in response to

being executed result in a computing device transferring an authenticated code

module to a cache memory of a processor; and executing the authenticated code

module from the cache memory in response to determining that the authenticated

code module stored in the cache memory is authentic.

Davis appears to disclose transferring BIOS code from a BIOS device 170_1 to

a cryptographic device 410 (Davis, col. 5, lines 55-65). Davis further appears to

disclose authenticating the received BIOS code (Davis, col. 5, line 66 through col. 6,

line 13). However, Davis appears to teach executing the authenticated BIOS code

from the BIOS device 170_1 instead of a cache memory as required by claims 29-34

(Davis, col. 6, lines 20-30). As a result, Davis is susceptible to an attack which

changes the BIOS code stored in the BIOS device 170_1 after the cryptographic

device 410 determined the BIOS code was authentic. While the window between

when the cryptographic device 410 determines the BIOS code is authentic and when

the processor completes execution of the BIOS code may be small, there is still a chance for an attacker to change the BIOS code during this window and thus compromise the system.

The invention of claims 29-34 may thwart such an attack by transferring the authenticated code module to a cache memory and executing the authenticated code module from the cache memory. Since the Davis does not appear to teach transferring the authenticated code module to a cache memory and executing the authenticated code module from the cache memory, Davis does not anticipate claims 29-34. Applicant respectfully requests the rejection of claims 29-34 be withdrawn.

Claim Rejections - 35 USC § 102 (England)

The Official Action rejected claims 1-34 under 35 USC 102(e) as being anticipated by England et al (US 6,651,171). Applicant has canceled claims 1, 14 and 19-21 and amended claims 3, 6-8, 13, 15-18, 22, 25-29 and 31. Applicant respectfully requests the rejection of claims 2-13, 15-18, 22-23, and 25-34 withdrawn in light of the following.

Claims 2-13

As a result of the present amendment, each of claims 2-13 require *configuring a cache memory of a processor to operate as a random access memory*, transferring an authenticated code module to the cache memory of the processor, authenticating the authentic code module storing in the cache memory, and *executing the authenticated code module from the cache memory operating as a random access memory* in response to determining that the authenticated code module stored in the cache memory is authentic.

The Official Action appears to rely on col. 8 lines 15-33 of England which describe a microprocessor 300. While England indicates that microprocessor 300 includes execution units 310, register files 320, cache 330 and addressable memory 340, Applicant is unable to locate any teaching in England regarding configuring the cache 330 of the microprocessor 300 as a random access memory and executing the authenticated code module from the cache 330 operating as a random access memory. Applicant believes the Official Action may be relying particularly on England at col. 8, lines 24-33 which describes internal addressable memory 340 and how the curtained memory rings can be partly or totally contained within memory 340. However, Applicant respectfully points out this section refers merely to internal addressable memory 340 which is separate and distinct from the cache 330. See, England Fig. 3. England does not appear to provide any teaching regarding containing the curtained memory rings in the cache 330 and from the perspective of claims 2-13 appears to provide no teaching regarding configuring the cache memory of a processor as a random access memory and executing the authenticated code module from the cache memory. Accordingly, England does not appear to anticipate the invention of claims 2-13. Applicant respectfully requests the withdrawal of the present rejection.

<u>Claims 15-18</u>

Claim 15 has been rewritten in independent form to include the limitations of all claims from which claim 15 depends. Accordingly, the scope of claim 15 is unchanged with the present amendment. Claims 16-18 have been amended to depend from claim 15. Accordingly, due to the present amendment, each of claims

15-18 require a chipset comprises a memory controller coupled to a memory and a separate private memory controller coupled to a private memory.

The Official Action appears to rely on col. 6, lines 5-67 of England for a teaching of a chipset comprising a memory controller and a separate private memory controller. Applicant has carefully reviewed col. 6, lines 5-67 of England. However, the cited section appears to merely describe a symbolic map of a memory space 200 and in particular the hierarchy of rings 210, 220 and 230 of FIG. 2. There appears to be no disclosure related to chipsets, memory controllers, and private memory controllers. Applicant respectfully requests the present rejection of claims 15-18 be withdrawn.

If the Examiner elects to maintain the present rejection, Applicant respectfully requests the Examiner to identify with more specificity (e.g. column, line and reference number) what in England is being relied upon for the teaching of a chipset, a memory controller, and private memory controller and in particular to a chipset comprising both a memory controller and a separate private memory controller.

Claims 22-23

Claim 22 has been rewritten in independent form to include the limitations of all claims from which claim 22 depends. Accordingly, the scope of claim 22 is unchanged with the present amendment. Claim 23 has been amended to depend from claim 22. Accordingly, due to the present amendment, each of claims 22-23 require a processor to transfer the authenticated code module from a machine readable medium interface to a private memory of the processor and to execute the authenticated code module stored in the private memory after authenticating the

authenticated code module, *wherein the private memory comprises internal cache memory of the processor.*

As mentioned above in regard to claims 2-13, England does not appear to teach using an internal cache memory as a private memory and thus does not anticipate the invention of claims 22-23. Applicant respectfully requests the rejection of claims 22-23 be withdrawn.

Claims 25-28

Claim 25 has been rewritten in independent form to include the limitations of all claims from which claim 25 depends. Accordingly, the scope of claim 25 is unchanged with the present amendment. Claims 26-28 have been amended to depend from claim 25. Accordingly, due to the present amendment, each of claims 25-28 require a chipset comprises a memory controller coupled to a memory and a separate private memory controller coupled to a private memory. As mentioned above in regard to claims 15-18, England does not appear to teach a chipset comprising both a memory controller and a separate private memory controller. England therefore does not anticipate the invention of claims 25-28. Applicant respectfully requests the present rejection be withdrawn.

Claims 29-34

As a result of the present amendment, each of claims 29-34 require a machine readable medium comprising one or more instructions that in response to being executed result in a computing device transferring an authenticated code module to a cache memory of a processor, and executing the authenticated code module from the cache memory. As mentioned above in regard to claims 2-13, England does not appear to teach transferring an authenticated code module to a
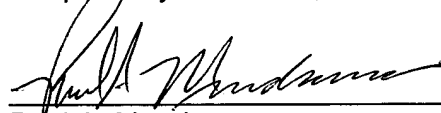
cache memory of a processor and executing the authenticated code module from the

cache memory. Applicant therefore requests the present rejection be withdrawn.

Conclusion

The foregoing is submitted as a full and complete response to the Official Action. Applicant submits that all remaining claims are in condition for allowance. Reconsideration is requested, and allowance of all remaining claims is earnestly solicited.

Should it be determined that an additional fee is due under 37 CFR §§1.16 or 1.17, or any excess fee has been received, please charge that fee or credit the amount of overcharge to deposit account #02-2666. If the Examiner believes that there are any informalities which can be corrected by an Examiner's amendment, a telephone call to the undersigned at (503) 439-8778 is respectfully solicited.

Respectfully submitted,

Paul A. Mendonsa
Reg. No. 42,879

BLAKELY SOKOLOFF TAYLOR & ZAFMAN, LLP
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(503) 439-8778